

Peter A Clarke

Australian websites attacked by a cryptojacking attack....

February 12, 2018 |

There is a positive in all of the attacks in cyberspace... the English vocabulary has grown and become enriched by new terms. Ever heard of cyrpojacking. It is a form of malware (another gift to the mother tongue to describe malicious software) which forces computers to mine cryptocurrency which generates profits for the hacker. Australian Government sites have been successfully breached through a browser plug in provided by a third party. Hackers inserted Coinhive into the plug in which hijacked the processing Third Party vulnerabilities are a chronic problem for businesses and government because their internal controls are not easily supervised and audited but their services are necessary.

The Guardian in [Cryptojacking attack hits Australian government websites](#) reports that in Australia the Victorian Parliament website has been compromised as has the Queensland Ombudsman, the City of Casey and the South Australian City of Unley Council. These types of breaches highlight which organisation and agencies have been less diligent with their data security.

Stay Smart Online put out an advisory today stating:

Crypto-mining threat for business

What's happened?

Thousands of websites across the globe have fallen victim to crypto-mining malware, after using a popular web tool designed to help people with vision impairment, dyslexia and low literacy.

In crypto-mining, the power and memory of your computer is used to generate cryptocurrency. If criminals gain access to your computer they can generate crypto-currency without your knowledge.

Security researcher Scott Helme claims 4,275 websites have been hijacked worldwide, including in Australia.

It is understood criminals secretly added a malicious program onto the website plug-in 'Browsealoud' which allowed them to mine cryptocurrency when the browser window was loaded.

Does it affect my business?

Businesses that rely on the digital accessibility tool 'Browsealoud' to deliver a text-to-speech web application are potentially affected.

Texthelp, the company that delivers 'Browsealoud' says it has taken the program offline while the company alerts its customers.

What do I need to do?

- Install any security updates as they become available.
- Make sure your organisation's computers and applications are up to date.

The Guardian article provides:

A series of Australian government websites, including the Victorian parliament's, have been compromised by malware that forces visitors' computers to secretly mine cryptocurrency, as part of a worldwide security breach.

The process, [known as cryptojacking](#), forces a user's computer to mine cryptocurrency without their permission, generating profits for the hacker.

Government websites were infected with the malware on Sunday after a browser plug-in made by a third-party was compromised. Thousands of sites, including the UK's National Health Service, and the UK's own data protection watchdog, [were affected](#).

In Australia the cryptojacking attack hit the official website of the Victorian parliament, the Queensland Civil and Administrative Tribunal, the Queensland ombudsman, the Queensland Community Legal Centre homepage, and the [Queensland](#) legislation website, which lists all of the state's acts and bills.

Hackers exploited a vulnerability in the popular browser plug-in Browsealoud, a program that converts website text to audio for visually impaired users.

The makers of Browsealoud, Texthelp, [confirmed that hackers inserted a script known as Coinhive](#) into their software. Coinhive hijacks the processing power of a user's computer to mine the cryptocurrency Monero.

On Monday morning, Texthelp took the Browsealoud plugin offline, which meant that new visitors to the affected sites would no longer load the cryptojacking script.

At the time of publication on Monday, the Queensland legislation website had taken the further step of removing the Browsealoud script entirely, but it remained on the sites of the Victorian parliament, QCAT and the Queensland ombudsman. On Monday afternoon QCAT contacted the Guardian to say it had removed the script from its website.

Scott Helme, a UK-based security researcher [who discovered the malware](#), said government websites could have done more to prevent the attack.

"When you load software like this from a third party, that third party can change it and make it do whatever they want," he said. "There are easy ways to make sure they don't do that.

"We don't know how Texthelp were compromised yet, so it is hard to say whether they were really unlucky or there was some kind of inherent problem with what they were doing.

"But there were ways the government sites could have protected themselves from this. It may have been difficult for a small website, but I would have thought on a government website we should have expected these defence mechanisms to be in place."

Helme [documented the attack](#) on his website, while Texthelp said an investigation was under way.

“The company has examined the affected file thoroughly and can confirm that it did not redirect any data, it simply used the computers’ CPUs to attempt to generate cryptocurrency,” it said.

“The exploit was active for a period of four hours on Sunday. The Browsealoud service has been temporarily taken offline and the security breach has already been addressed, however Browsealoud will remain offline until Tuesday 12.00 GMT.”

Other government sites affected include Victoria’s City of Casey council, Western Australia’s City of Bayswater council, South Australia’s City of Unley council, and the office of the Queensland Public Guardian, which protects the rights of young children in care.

In December the Guardian reported that [nearly 1 billion visitors](#) to the video sites Openload, Streamango, Rapidvideo and OnlineVideoConverter were also being cryptojacked.

The office of the Queensland Parliamentary Council, which operates the Queensland legislation website, and the Victorian parliament have been contacted for comment.

Tennessee has also been affected with the Decatur County General Hospital having to notify 26,000 patients of a data breach. The [notice provides](#):

Decatur County General Hospital takes the privacy and security of its patients’ health information seriously. We are writing to let you know about an incident involving an electronic medical record (EMR) system used by our hospital. On November 27, 2017, we received a security incident report from our EMR system vendor indicating that unauthorized software had been installed on the server the vendor supports on our behalf. The unauthorized software was installed to generate digital currency, more commonly known as “cryptocurrency.” Following receipt of the incident report, we began our own investigation into the incident. At this time, our investigation continues, but we believe an unauthorized individual remotely accessed the server where the EMR system stores patient information to install the unauthorized software. The software was installed on the system at least as of September 22, 2017, and the EMR vendor replaced the server and operating about four days later.

Over the past several months, there have been numerous news stories about computer systems around the country being affected by similar incidents involving the unauthorized installation of this type of software. Again, while our investigation continues into this matter, we have no evidence that your information was actually acquired or viewed by an unauthorized individual, and based upon reports of similar incidents, we do not believe that your health information was targeted by any unauthorized individual installing the software on the server. Our investigation to date, however, has been unable to reasonably verify that there was not unauthorized access of your information. Information contained on the affected server included demographic information such as patient names, addresses, dates of birth, and Social Security numbers, clinical information such as diagnosis and treatment information, and other information such as insurance billing information.

Complimentary Credit Monitoring Service

As a safeguard, we have arranged for online credit monitoring service (myTrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies, at no cost to affected patients. If you have been a patient at Decatur County General Hospital, please call 1-877-760-4702 to see if you are eligible.

Directions for Placing a Fraud Alert

Additionally, you may choose to adopt an increased level of protection by placing a fraud alert on your credit file at the three major credit bureaus. A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. An initial fraud alert lasts 90 days. You may also place a security freeze, or credit freeze, on your credit file which is designed to prevent credit, loans, and services from being provided in your name without consent. However, setting a security freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift

and/or remove a credit freeze. Credit freeze laws vary from state to state. Contact information for the three major bureaus is provided below:

.....

As a general matter, you should remain vigilant by regularly reviewing financial account, medical bills and health insurance statements, such as explanations of benefits (EOB). The Federal Trade Commission (FTC) recommends that you check your credit reports periodically to help spot problems. You can obtain a free credit report annually from each of the three major credit bureaus by calling 1-877-322-8228 or by visiting www.AnnualCreditReport.com. You should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the FTC. For more information about identity theft and other forms of financial fraud, as well as information about fraud alerts and security freezes, you can contact the FTC online at www.ftc.gov/idtheft, by mail at Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, or by calling 1-877-ID-THEFT (438-4338).

Regularly monitoring financial and other account activity and periodically obtaining and reviewing credit reports are prudent steps to take given the prevalence of identity theft and related crimes.

Again, our investigation into this incident continues but we do not believe the motivation of any unauthorized access to the EMR server was to access or acquire your information. We encourage you, however, to exercise caution regarding communications if you receive an unsolicited call or email about this incident. Please know that we will not call or email anyone requesting any personal information as a result of this situation.

We take protecting our patients' information seriously, and we regret any inconvenience or concern this unfortunate incident has caused you. Decatur County General Hospital has set up a dedicated number for you to call with any questions or for more information. Should you have any questions, please do not hesitate to call 1-877-760-4702, Monday through Friday (except holidays), 8:00 am to 8:00 pm Central Time.

Like 0



One Response to “Australian websites attacked by a cryptojacking attack....”

1. [Australian websites attacked by a cryptojacking attack.... | Australian Law Blogs](#) February 12th, 2018

[...] Australian websites attacked by a cryptojacking attack.... [...]

Leave a Reply

Name (required)

Mail (will not be published) (required)

Website

Your comments

Submit Comment

Copyright © 2008/2009 Peter A. Clarke All Rights Reserved. [Login](#) | [RSS](#)